# AFFIDAVIT OF
# SPECIAL AGENT BRIAN CHRISTIANSEN

I, Brian Christiansen, declare and state the following:

## INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Secret Service ("USSS") and have been employed as such since August of 2021. I attended the United States Secret Service Special Agent Training Course at the James J. Rowley Training Center in Beltsville, Maryland. I am currently assigned to the Boston Field Office where I conduct financial crime investigations, including investigations of violations of 18 U.S.C. § 1343 (Wire Fraud). In connection with these investigations, I have conducted or participated in numerous field interviews of suspects and witnesses, electronic and physical surveillance, researched bank account documents and documents relating to the wiring of monies between banks. Through my training and experience, I have become familiar with various financial frauds and schemes such as bank frauds, wire frauds and mail frauds.

## PURPOSE OF AFFIDAVIT

2. I submit this affidavit in support of a Verified Complaint for Forfeiture *in Rem* against the following assets:

a. 87,637.000 USDT seized from a Binance account with user ID XXXX1716 on or about May 24, 2023 (the "Defendant Cryptocurrency" and "BINANCE ACCOUNT").[1]

3. As set forth below, there is probable cause to believe that the Defendant Cryptocurrency is traceable to and/or involved in a cryptocurrency investment fraud scheme that targeted an individual located in Millis, Massachusetts. The scheme duped the individual into

[1] USDT (Tether) is a form of cryptocurrency, described in more detail below.

completing transfers totaling $975,900 in United States currency from his personal bank account into his Crypto.com account and then portions of which were ultimately transferred into the BINANCE ACCOUNT.

4. Accordingly, there is probable cause to believe that the Defendant Cryptocurrency is property, real or personal, which constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1343 (Wire Fraud), and therefore is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C). The Defendant Cryptocurrency was seized pursuant to a seizure warrant issued in the District of Massachusetts.

5. This affidavit is based on my personal knowledge, information provided by other law enforcement offices and government employees, and information gathered during this investigation including interviews of witnesses, the review of documents, and conversations with other law enforcement officers. This affidavit is not intended to set forth all of the information that I have learned during this investigation but includes only the information necessary to establish probable cause.

## FORFEITURE AUTHORITY

6. Under 18 U.S.C. § 981(a)(1)(C), property, real or personal, which constitutes or is derived from proceeds traceable to a violation of a specified unlawful activity, specifically violations of 18 U.S.C. § 1343 (Wire Fraud), is subject to civil forfeiture. Pursuant to 18 U.S.C. § 1961(1), as incorporated by 18 U.S.C. § 1956(c)(7)(A), violations of 18 U.S.C. § 1343 are a specified unlawful activity.

## BACKGROUND ON CRYPTOCURRENCY

7. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

8. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies.[2] Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[3] Cryptocurrency is not illegal in the United States.

9. Tether ("USDT") is an alternative type of cryptocurrency or altcoin token. Payments or transfers of value made with Tether are recorded in the blockchain network, but unlike decentralized cryptocurrencies like Bitcoin, Tether has some anatomical features of centralization. One centralized feature is that Tether is a stablecoin or a fiat-collateralized token that is backed by fiat currencies, or currencies issued by governments like the dollar and euro.

[2] Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

[3] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

Tether is backed with a matching one to one fiat amount, making it much less volatile than its counterpart, Bitcoin.

10. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers, 26–36 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

11. Although cryptocurrencies such as Bitcoin and Tether have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes, such as money laundering, and is an oft-used means of payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track transactions.

12. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a

smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange.

13. Cryptocurrency "exchangers" and "exchanges" are individuals or companies that exchange cryptocurrencies for other currencies, including U.S. dollars. According to Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.[4] Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account.

14. Binance Capital Management Co., Ltd. ("BINANCE") is a cryptocurrency exchange and custodian that allows users to buy, sell and store digital assets. They hold a Money Service Business Registration in the United States. Their registration shows an address of P.O. Box 472, Harbour Place, 2nd Floor, North Wing, 103 South Church Street, George Town, Grand Cayman, KY1-1106.

[4] *See* "Application of FinCEN's Regulations to Person Administering, Exchanging, or Using Virtual Currencies," *available at* https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

## PROBABLE CAUSE

### *The Scheme to Defraud*

15. On November 4, 2022, Victim-1 of Millis, Massachusetts contacted the USSS Boston Field Office providing information indicating he was the victim of a cryptocurrency trading scam. Victim-1 explained that he was initially contacted on August 15, 2022, through text message by phone number XXXXXXX2417. The text message was looking for an individual named "Chad", to which Victim-1 replied saying that they have the wrong number. This number then began a conversation with Victim-1, telling him that he seemed like a nice person and began asking personal questions.

16. After the initial text message received by Victim-1, the phone number then asked Victim-1 to download a messaging application called WhatsApp, so they could continue to communicate. Victim-1 installed WhatsApp and began communication through this application with phone number XXXXXXX8939. Victim-1 stated that all communications from this point forward were through the WhatsApp application.

17. Victim-1 stated that the conversation progressed over several days and he was told that the individual he was communicating with was named "Li YU". YU explained to Victim-1 that she worked for Company-1 as the office manager out of their Manhattan, New York location.[5] Victim-1 mentioned to YU that he just retired, and YU became very interested in retirement. YU began to ask Victim-1 questions regarding how much money she would need to retire and what type of investments he had for retirement. Victim-1 stated that it felt like a normal conversation with YU, and Victim-1 became trusting and emotionally attached to YU through the weeks of conversation.

[5] Company-1 has no record of this employee.

18. Victim-1 said that after a few days of conversation, YU began to talk about cryptocurrency investing. YU explained to Victim-1 that she invests all her money into cryptocurrency and told Victim-1 that her uncle is retired from Goldman Sachs, but still has a team of analysts that he works with in the cryptocurrency market. YU further told Victim-1 that her uncle's team of analysts analyze the market 24 hours a day and look for "trading signals" that they trade cryptocurrency on for "good profits". Victim-1 stated that YU then offered to teach him about investing and trading cryptocurrency, which Victim-1 accepted. Before he began communicating with YU, Victim-1 had never purchased or sold cryptocurrency and knew nothing about cryptocurrency.

19. Victim-1 stated that after he agreed to learn about cryptocurrency from YU, they texted everyday through WhatsApp. YU introduced Victim-1 to cryptocurrency exchanges such as Crypto.com and Coinbase.

20. On or about August 23, 2022, Victim-1 stated that YU helped him set up an account with Crypto.com, Coinbase, and "comexnar.com". Victim-1 said that he followed instructions from YU to set up each of these accounts. YU instructed Victim-1 to put his U.S. fiat into his Coinbase account and exchange it for USDC (a stablecoin also known as USD Coin). From here, YU explained to Victim-1 that he could then invest that USDC into his "Comex" account, an account that YU specifically directed and helped Victim-1 open. Victim-1 showed screenshots from WhatsApp of the messages that YU sent him, showing instructions on how to open an account with Comex.

21. On or about August 23, 2022, Victim-1 made his first transfer of 3,000 USDC from his Crypto.com account into his Comex account, which he thought was a legitimate cryptocurrency exchange.

22. Victim-1 stated that YU sent him the website URL "https://comexbrs.com/h5" that he was to click on in order to download the Comex app. Following this, Victim-1 stated he followed the instructions, but was unable to download the "Comex" app on his iPhone. Since he was unable to download the app, Victim-1 stated that YU told him to use the website URL "https://comexnar.com/app" to access his account with Comex.

23. Victim-1 stated that YU told him he was looking at a profit of $1.3 million with the investments that he had in his Comex account.

24. At the end of October, Victim-1 stated that YU told him that trading would end for the year so that the analysts could finalize their portfolios for the year end "tax consequences." YU said she did not know when the trading would open again, but that Victim-1 had to contact customer support to see how much money he would have to pay in commissions. Victim-1 stated that customer service at Comex told him they would have to take $198,192 in United States currency for to pay commissions, which would come out of his $1.3 million in profit.

25. On or about October 27, 2022, Victim-1 attempted to withdraw funds from his Comex account. His first withdrawal attempt failed, so he contacted Comex customer service. Victim-1 stated that customer service told him that since he had over one million dollars total in his account, that he would have to pay approximately $200,000 in United States currency into his account to withdraw his funds. Victim-1 said he was confused by this, so asked YU about it and was told that it was part of Comex's security procedures. Victim-1 stated that he was skeptical, but since he had so much money tied up in his Comex account, he stated he paid the approximately $200,000 in United States currency on October 27, 2022. This was the final transfer that Victim-1 made into what he believed was his Comex account.

26. Shortly after his final transfer, Victim-1 attempted to move his funds from his Comex account to his Coinbase account so he could then transfer them to his personal bank account. Victim-1 saw that his funds left his Comex account, but the funds never showed up in his Coinbase account. Victim-1 contacted Coinbase customer support and provided them with the transaction hash and details. Coinbase informed Vicitm-1 that the address that the funds were coming from was an inauthentic address. From here, Victim-1 contacted the Comex customer support, and was told that the funds did not transfer to Coinbase because his credit score with Comex was too low. After hearing this, Victim-1 did not transfer any more of his money and started to research cryptocurrency scams. Victim-1 stated that his money disappeared from his Comex account, and he does not know where his funds went.

27. Between August 23, 2022 and October 27, 2022, Victim-1 made a total of thirteen (13) transfers totaling $975,900 from his Crypto.com account into his Comex account. All thirteen (13) transfers totaling 975,770 USDC transferred from his Crypto.com account into wallet address 0x64f09a1a30cf824d8da994be97829f4fc6a0892b, which Victim-1 believed to be linked to his Comex account.

***The Comex URL Appears to Be Fraudulent***

28. Vicitm-1 provided screenshots of the Comex trading platform that he visited using the website URL "https://comexnar.com/app". Screenshots provided by Victim-1 appear to indicate gains, losses, and transfer history of cryptocurrency.

29. I conducted a thorough open-source search for "https://comexnar.com/app" and was unable to find the website that Victim-1 used. Based on my training and experience, as well as conversations with other investigators familiar with cryptocurrency platforms, I would expect a legitimate cryptocurrency platform website to display clearly outlined platform policies,

company contact information, information regarding the platform's creation, company staff information, along with access for desktop and mobile computing.

30. Further, while conducting an open-source search, several "scamwatcher" websites flagged comexnar.com as being "unsafe," I found that the domain was created on August 13, 2022, which seems suspicious since the first text that Victim-1 received from YU was on August 15, 2022.

31. When attempting to navigate to this website utilizing a Microsoft Edge web browser, I receive an error message that indicates the domain is not registered.

32. During the course of my investigation, I was not able identify or determine an address for the company headquarters. I also was not able to identify any employees shown on the website. Additionally, I did not identify any privacy policy posted on the website nor any type of webpage indicating regulatory oversight or additional tabs showing career opportunities to work for this company, as one would expect for a legitimate company.

33. In addition to these indications, when conducting open-source research on this website, I identified multiple websites indicating this website was a "scam". Another open-source report indicated this website had a "1% trust index", which reflects the trust in a website. The 1% trust index is the lowest score that can be given according to their algorithm.

34. Based on my training and experience, the discrepancies identified above are not typical for a legitimate cryptocurrency platform.

35. Accordingly, I have probable cause to the believe Victim-1 was fraudulently induced to transfer funds to a scam cryptocurrency platform, *i.e.*, wire fraud, in violation of 18 U.S.C. § 1343.

***The Flow of Funds***

36. Subsequent analysis indicates that the Defendant Cryptocurrency in the BINANCE ACCOUNT can be traced to the transfers from Victim-1's Crypto.com account.

37. The thirteen (13) transfers from Victim-1's account at Crypto.com are reflected in Figure 1 below, with times shown in UTC[6]:

| |
|---|
| **Date: 08-24-2022 01:48:05** |
| Amount USDC: 2990.00 |
| Sent to wallet address: 0x64f09a1a30cf824d8da994be97829f4fc6a0892b |
| Transaction Hash: 0x197677cfca32a72784b3fdc6ddc416bd69cbfe3cc4311f717ee5606d7d1326b3 |
| |
| **Date: 08-25-2022 18:45:29** |
| Amount USDC: 990.00 |
| Sent to wallet address: 0x64f09a1a30cf824d8da994be97829f4fc6a0892b |
| Transaction Hash: 0x6de921f353ca3bc168ed8453d8f2bd975afcabb57b99fcc2bccf83c587c0ef99 |
| |
| **Date: 08-27-2022 19:27:59** |
| Amount USDC: 2290.00 |
| Sent to wallet address: 0x64f09a1a30cf824d8da994be97829f4fc6a0892b |
| Transaction Hash: 0x0fc46c76ac3a5dce477cc3db24d0fb950d2257e32979f53b32460726cc5e7672 |
| |
| **Date: 08-31-2022 20:54:57** |
| Amount USDC: 61990.00 |
| Sent to wallet address:  0x64f09a1a30cf824d8da994be97829f4fc6a0892b |
| Transaction Hash: 0xff9899ab0319c71054a0132dc289c1bb3dfd2a04f72e4fefec9999c3423788b6 |
| |
| **Date: 09-09-2022 02:54:19** |
| Amount USDC: 39990.00 |
| Sent to wallet address: 0x64f09a1a30cf824d8da994be97829f4fc6a0892b |
| Transaction Hash: 0x575b8650318534a2dc567158c398fef09bab48ac5d976a1b28311771e7f287b9 |
| |
| **Date: 09-09-2022 12:27:21** |
| Amount USDC: 49990.00 |
| Sent to wallet address: 0x64f09a1a30cf824d8da994be97829f4fc6a0892b |
| Transaction Hash: 0xb6002fbeaa56ae8fd3d9f925d031ed87ca3391932854a132b44cad7df8d5cb10 |
| |
| **Date: 09-12-2022 22:46:39** |
| Amount USDC: 75990.00 |
| Sent to wallet address: 0x64f09a1a30cf824d8da994be97829f4fc6a0892b |

[6] UTC is Universal Time Coordinated, also known as Coordinated Universal Time. This is also known as Greenwich Mean Time.

| |
|---|
| Transaction Hash: 0x84726446d4eb06b6d1ab3e4cec517db6d12a62cc7bfa156f4105f409b0d09b72 |
| |
| **Date:09-19-2022 16:14:47** |
| Amount USDC: 149990.00 |
| Sent to wallet address: 0x64f09a1a30cf824d8da994be97829f4fc6a0892b |
| Transaction Hash: 0x86af8ee7da64a7e55618a929ac599597c840bce3581187c5a3908d6a760a5f86 |
| |
| **Date: 09-21-2022 20:18:47** |
| Amount USDC: 142990.00 |
| Sent to wallet address: 0x64f09a1a30cf824d8da994be97829f4fc6a0892b |
| Transaction Hash: 0xa68cfecf14bc4705e4be4b13f781186eb07ac737cf54a327a463e961f7fb5c56 |
| |
| **Date: 10-07-2022 12:11:59** |
| Amount USDC: 49990.00 |
| Sent to wallet address: 0x64f09a1a30cf824d8da994be97829f4fc6a0892b |
| Transaction Hash: 0xa375f8ea0f7c69316ef67dc536b0e09759d35f4573390d49545027a240353537 |
| |
| **Date: 10-18-2022 21:57:23** |
| Amount USDC: 149990.00 |
| Sent to wallet address: 0x64f09a1a30cf824d8da994be97829f4fc6a0892b |
| Transaction Hash: 0xcaabd5358cf5750db83a3903e7d08fd4eed9a58753534d458c42c4a936c33e1d |
| |
| **Date: 10-19-2022 22:46:59** |
| Amount USDC: 48490.00 |
| Sent to wallet address: 0x64f09a1a30cf824d8da994be97829f4fc6a0892b |
| Transaction Hash: 0x0b32765b2e68eb9b9b4fda9957207a4848ec99de609fa997723c721a58af6fd0 |
| |
| **Date: 10-28-2022 03:53:23** |
| Amount USDC:  200090.00 |
| Sent to wallet address: 0x64f09a1a30cf824d8da994be97829f4fc6a0892b **(Wallet ending in 0892b)** |
| Transaction Hash: 0x2a2afb4ba4120de2781db2772ec66d8e8ebfb795c0d6192fe5ae649e547c56ea |
| |

**Figure 1**

***<u>The Flow of Funds to BINANCE ACCOUNT</u>***

38. After receiving 975,900 USDC of Victim-1's funds from August 24 to October 28, 2022, the controller of **wallet address ending in 0829b** remitted 7 out of the 13 transactions almost immediately into the **wallet address ending in e6E15**. Intermediary wallets are typically private wallets or non-exchange wallets that obfuscate transactions on the blockchain. Intermediary wallets support the movement of illicitly obtained funds as they help to conceal and

disguise the source of the USDC by layering and severing straight line coordinates of transaction activity on the blockchain to cash out exchangers.

39. A listing of the transactions into the **wallet address ending in e6E15** involving Victim-1’s funds can be found in Figure 2 below, with times shown in UTC:

| |
|---|
| **Date: 08-25-2022 19:13:10** |
| Amount USDC: 990.00 |
| Sent to wallet address: 0x81CE629Bc840A5C17E2Ce37CC18F8e9483Be6E15 |
| Transaction Hash: 0x2aabe3f1976e780402994bec3a92a6f721d90b28a140321d041cd448b04c65e4 |
| |
| **Date: 08-27-2022 19:39:54** |
| Amount USDC: 2290.00 |
| Sent to wallet address: 0x81CE629Bc840A5C17E2Ce37CC18F8e9483Be6E15 |
| Transaction Hash: 0x2bf7bfae277492ba62eff4038e2e6aafaebb0300b8d077a244a158d767779c7e |
| |
| **Date: 08-31-2022 21:06:46** |
| Amount USDC: 61990.00 |
| Sent to wallet address: 0x81CE629Bc840A5C17E2Ce37CC18F8e9483Be6E15 |
| Transaction Hash: 0x16650078e03717830f012eb75f34a4b9b61340a9e22695120fca4e1fd132f8b7 |
| |
| **Date: 09-09-2022 03:26:24** |
| Amount USDC: 39990.00 |
| Sent to wallet address: 0x81CE629Bc840A5C17E2Ce37CC18F8e9483Be6E15 |
| Transaction Hash: 0xc3289acf0e91ba7007a96c328bfb395c35941a7194cee7be210394626853ca45 |
| |
| **Date: 09-09-2022 13:17:09** |
| Amount USDC: 49990.00 |
| Sent to wallet address: 0x81CE629Bc840A5C17E2Ce37CC18F8e9483Be6E15 |
| Transaction Hash: 0x615850ab0840a2eb626a0f346d29101b16a6396cd13f8065f63a19fd0b4b8fa1 |
| |
| **Date: 09-12-2022 23:12:41** |
| Amount USDC: 75990.00 |
| Sent to wallet address: 0x81CE629Bc840A5C17E2Ce37CC18F8e9483Be6E15 |
| Transaction Hash: 0xff62bb73da750d89bc7a2069d83ed32d16fcc271004e8581d2c4d18320f7e08c |
| |
| **Date: 09-19-2022 17:34:11** |
| Amount USDC: 149990.00 |
| Sent to wallet address: 0x81CE629Bc840A5C17E2Ce37CC18F8e9483Be6E15 **(Wallet ending in e6E15)** |
| Transaction Hash: 0xc8788f42a71e8df54e62cbc40d0b0fea7ac616d69794b302b9665b0a16a2f8da |

**Figure 2**

40. After receiving approximately 381,230 USDC in Victim-1's funds from August 25 – September 19, 2022, (*see* Figure 2), the controller of **wallet address ending in e6E15** remitted most of the funds into **wallet address ending in fCd0f**. Before the funds were received into **wallet address ending in fCd0f**, the controller of the **wallet address ending in e6E15** converted the USDC into DAI. DAI is an alternate type of cryptocurrency and a decentralized stablecoin.

41. A listing of these transactions can be found in Figure 3 below, with times shown in UTC:

| |
|---|
| **Date: 08-31-2022 21:13:22** |
| Amount DAI: 61,963.673544550888 |
| Sent to wallet address: 0x29cfeeeCCddC76ac7B6684dA7E6E8Ee7f32fCd0f |
| Transaction Hash: 0x71af9e1bf4f54b5d9b3166b409f6db7816d36715e76e0e1ecafbeb73aefd18ac |
| |
| **Date: 09-09-2022 03:41:16** |
| Amount DAI: 59,950.800718781418772824 |
| Sent to wallet address: 0x29cfeeeCCddC76ac7B6684dA7E6E8Ee7f32fCd0f |
| Transaction Hash: 0x9d35f4171f9273c1222ad8dbb39da638027bfc7faa54af4d145d597b28980f7f |
| |
| **Date: 09-12-2022 23:25:11** |
| Amount DAI: 76,945.8703460958 |
| Sent to wallet address: 0x29cfeeeCCddC76ac7B6684dA7E6E8Ee7f32fCd0f |
| Transaction Hash: 0x679823373e64e6297844d3adb5ed959d2fa007a5b31b24fb350405405c1182e9 |
| |
| **Date: 09-19-2022 18:02:11** |
| Amount DAI: 149,912.51166643332 |
| Sent to wallet address: 0x29cfeeeCCddC76ac7B6684dA7E6E8Ee7f32fCd0f **(Wallet ending in fCd0f)** |
| Transaction Hash: 0x069ee26a8dddfe27d8911c78219182c691b641a7874212468a6a9dd893e652bf |

**Figure 3**

42. After receiving approximately 348,736.27949 DAI in Victim-1's funds between August 31 and September 19, 2022 (*see* Figure 3), the controller of **wallet address ending in fCd0f** remitted the funds to a **wallet address ending in DA4C5**. There was a total of three (3) transactions, as shown in Figure 4, which contained a combined approximately 2,245,166 DAI. The number of DAI moved here is more than Victim-1's funds, which tells me that there are

other victim's funds contained in the **wallet address ending in fCd0f**. This tactic is done to attempt to conceal and disguise the sources of the DAI.

43. A listing of these transactions can be found in Figure 4 below, with times shown in UTC:

| |
|---|
| **Date: 09-01-2022 06:34:17** |
| Amount DAI: 696,988.00 |
| Sent to wallet address: 0xd278e49e6cb2C34F672782845F3C9A6A727DA4C5 |
| Transaction Hash: 0x0d268387737aaad7eb7a43e0e05bb4207994eb58e49d4955f002d2f86a593d55 |
| |
| **Date: 09-09-2022 11:18:03** |
| Amount DAI: 770,193.00 |
| Sent to wallet address: 0xd278e49e6cb2C34F672782845F3C9A6A727DA4C5 |
| Transaction Hash: 0x62cabae94f5ea4b750b8507445fb56c28b3a8c97df0d9657e46e28d23dd2f98c |
| |
| **Date: 09-13-2022 15:35:57** |
| Amount DAI: 778,211.00 |
| Sent to wallet address: 0xd278e49e6cb2C34F672782845F3C9A6A727DA4C5 **(Wallet ending in DA4C5)** |
| Transaction Hash: 0x4d44edbb27fc6249153ace3a8f1100d04da5ea24ba3798e1a7972fbdd38b4b6a |

**Figure 4**

44. After receiving approximately 2,245,166 DAI, the controller of **wallet address ending in DA4C5** remitted a portion of the funds to a **wallet address ending in f8e64**. This was done in one (1) transaction where 896,611 DAI were moved.

45. A listing of these transactions can be found in Figure 5 below, with times shown in UTC:

| |
|---|
| **Date: 09-13-2022 17:17:51** |
| Amount DAI: 896,611.00 |
| Sent to wallet address: 0x1B8eeB6885382F3e10DACfAd40ae92E2732f8e64 **(Wallet ending in f8e64)** |
| Transaction Hash: 0xd5692b2ce213563108c0dad111c64601c9835249b482b18b8ea369a87c8a45e1 |

**Figure 5**

46. After receiving approximately 896,611 DAI, the controller of **wallet address ending in f8e64** remitted funds containing Victim-1's to a **wallet address ending in CF775**.

Before sending the USDT, the controller of **wallet address ending in f8e64** exchanged the DAI for USDT.

47. A listing of these transactions can be found in Figure 6 below, with times shown in UTC:

| |
|---|
| **Date: 10-14-2022 08:26:23** |
| Amount USDT: 999,869 |
| Sent to wallet address: 0x14C145659De2Cad8FfAfC7DA519068eb421CF775 |
| Transaction Hash: 0x9b8e311a23eff8b078c4810bdba45cfa951771e3250ed5ec381a10f383491c92 |
| |
| **Date: 10-14-2022 08:29:59** |
| Amount USDT: 999,863 |
| Sent to wallet address: 0x14C145659De2Cad8FfAfC7DA519068eb421CF775 |
| Transaction Hash: 0xe7985ab7583d6d6ca2ba5b7bbd22f819adbd0bc9c9af02413dc3699a9d0b1e7c |
| |
| **Date: 10-14-2022 08:32:35** |
| Amount USDT: 489,532 |
| Sent to wallet address: 0x14C145659De2Cad8FfAfC7DA519068eb421CF775 **(Wallet ending in CF775)** |
| Transaction Hash: 0x9353ffc4ce4e0b24048b7bd76d85d49f1bcb8369ca974b089f33dd59da8c487c |

**Figure 6**

48. After receiving approximately 2,489,264 USDT, the controller of **wallet address ending in CF775** remitted funds containing Victim-1's to a **wallet address ending in BF4B0**.

49. A listing of these transactions can be found in Figure 7 below, with times shown in UTC:

| |
|---|
| **Date: 10-14-2022 08:47:35** |
| Amount USDT: 3,524,603.00 |
| Sent to wallet address: 0x5248a851207b4654D8EE8c04c39687cf28fBF4B0 **(Wallet ending in BF4B0)** |
| Transaction Hash: 0x32304bc45e14504f220f9817e5e5f47f8ce4cdac478af18b5c7926997f0986ee |

**Figure 7**

50. After receiving approximately 3,524,603 USDT, the controller of **wallet address ending in BF4B0** remitted funds containing Victim-1's to a **wallet address ending in 1f074**.

51. A listing of these transactions can be found in Figure 8 below, with times shown in UTC:

| |
|---|
| **Date: 10-14-2022 10:16:59** |
| Amount USDT: 500,000 |
| Sent to wallet address: 0x2CCF46E75ab9dB2D0ECA74443E57e55673A1f074 |
| Transaction Hash: 0xde25aafee67e0d36ddf73ba9707fbf0b7b5be1c87c9a3bd7477eeb6f60ab1148 |
| |
| **Date: 10-15-2022 18:20:23** |
| Amount USDT: 700,771 |
| Sent to wallet address: 0x2CCF46E75ab9dB2D0ECA74443E57e55673A1f074 |
| Transaction Hash: 0xc0f3d5a983d4c5af86aa9f0116f10b0f782f5518a2287c4c105d3f3bc1cdbc5f |
| |
| **Date: 10-16-2022 12:56:23** |
| Amount USDT: 300,000 |
| Sent to wallet address: 0x2CCF46E75ab9dB2D0ECA74443E57e55673A1f074 |
| Transaction Hash: 0x0597026120e9d15546f879542333288f68e1956c3a8a7cb92d26dc35b9afc4a5 |
| |
| **Date: 10-16-2022 15:19:35** |
| Amount USDT: 1,101,541 |
| Sent to wallet address: 0x2CCF46E75ab9dB2D0ECA74443E57e55673A1f074 **(Wallet ending in 1f074)** |
| Transaction Hash: 0x1936b57bb358092039436a41ccd25870461751a588f278cfa5c26607d49e870c |

**Figure 8**

52. After receiving approximately 2,602,312 USDT, the controller of **wallet address ending in 1f074** remitted funds containing Victim-1's to a **wallet address ending in 5CD6E.**

53. A listing of these transactions can be found in Figure 9 below, with times shown in UTC:

| |
|---|
| **Date: 10-15-2022 18:23:11** |
| Amount USDT: 80,000 |
| Sent to wallet address: 0xD732aAfa62762FD0d060Ba4Bd8aC90C11065CD6E |
| Transaction Hash: 0xd68e763f208a1c65074e83bcf7a67c1a4070f31b1f03da71b60d0773bfdb6398 |
| |
| **Date: 10-16-2022 06:00:59** |
| Amount USDT: 71,933 |
| Sent to wallet address: 0xD732aAfa62762FD0d060Ba4Bd8aC90C11065CD6E |
| Transaction Hash: 0x90ed882d5219b410bad0c89dc82e2552fb271f4cf7efee8c2e38474ac8aebce7 |
| |
| **Date: 10-16-2022 17:47:47** |
| Amount USDT: 100,000 |
| Sent to wallet address: 0xD732aAfa62762FD0d060Ba4Bd8aC90C11065CD6E **(Wallet ending in 5CD6E)** |
| Transaction Hash: 0xa590f017018f97e78a91ad6b82a78f13cda3d3dba04e3834b2d8469a0ede7113 |

**Figure 9**

54. After receiving approximately 251,933 USDT, the controller of **wallet address ending in 5CD6E** remitted funds containing Victim-1's to a **wallet address ending in 33F79**.

55. A listing of these transactions can be found in Figure 10 below, with times shown in UTC:

| |
|---|
| **Date: 10-16-2022 03:18:47** |
| Amount USDT: 35,249 |
| Sent to wallet address: 0xC3f537d4b9609A605528d231fa043b3e8D433F79 |
| Transaction Hash: 0x3ce3062efc0b5ba4f533daa5ea3f4ed817ef90fc7448a030cbdb97aeafb82fb9 |
| |
| **Date: 10-16-2022 15:03:59** |
| Amount USDT: 52,398 |
| Sent to wallet address: 0xC3f537d4b9609A605528d231fa043b3e8D433F79 **(Wallet ending in 33F79)** |
| Transaction Hash: 0xebe38052e2acd06cf0e4390d8bdd61b53865db7dfabd265b97632e98d9c30a54 |

**Figure 10**

56. After receiving approximately 87,647 USDT, the controller of **wallet address ending in 33F79** remitted funds containing Vicitm-1's to a **wallet address ending in 0A613**. The controller of **wallet address ending in 0A613** then sent funds containing Victim-1's to a **wallet address ending in 8B19F**. The controller of **wallett address ending in 8B19F** then sent approximately 340,136 USDT to a **wallet address ending in 5ADF2**.

57. A listing of these transactions can be found in Figure 11 below, with times shown in UTC:

| |
|---|
| **Date: 10-16-2022 15:50:11** |
| Amount USDT: 407,617.93 |
| Sent to wallet address: 0xF5e3B7ef2E8b90d6c5449dD03c6743e70a90A613 **(Wallet ending in 0A613)** |
| Transaction Hash: 0x0ef5564ed3d5043d7b8fb2cd6b993eb4337ab06d6f35ef1f27982f76806a86f7 |
| |
| **Date: 10-17-2022 02:55:59** |
| Amount USDT: 407,617.93 |
| Sent to wallet address: 0x5ff9Dc675d103b802D9F974774C8aA4457f8B19F **(Wallet ending in 8B19F)** |
| Transaction Hash: 0xe27a64f994be44a36c8f6dd7c2710a4345bd050883c600121eb74ad3d0f94850 |
| |
| **Date: 10-17-2022 06:10:23** |
| Amount USDT: 340,136 |
| Sent to wallet address: 0xA50da99F13Eaa5A703F05D51b203a78D2b05ADF2 **(Wallet ending in 5ADF2)** |

| |
|---|
| Transaction Hash: 0xf1fe4b582e8518ffa5242fbd361ce8e97a3802aa7229ea7804729cd38cd2de70 |

**Figure 11**

58. After receiving approximately 340,136 USDT, the controller of **wallet address ending in 5ADF2** remitted funds containing Vicitm-1's to BINANCE ACCOUNT.

59. A listing of these transactions can be found in Figure 12 below, with times shown in UTC:

| |
|---|
| **Date: 10-17-2022 11:56:23** |
| Amount USDT: 350,000 |
| Sent to wallet address: 0x13d56FC843E336e931C4bEE555271F5840180A49 **(Wallet ending in 80A49)** |
| Transaction Hash: 0xd9ba6a0c800ea5e1cd4445046a09acb37450081d040b9516b7690b0f10c6a13e |

**Figure 12**

60. A visual depiction containing the transfers identified in Figures 1 through 12 above, are reflected in Attachment A.

61. After reviewing Attachment A and other facts of this investigation, I was able to identify that after multiple intermediary transfers, up to 87,637.00 USDT of Victim-1's funds were ultimately transferred to **wallet address ending in 80A49**.

62. Records reflect that the transfer of Victim-1's funds into **wallet address ending in 80A49** (referenced in Figures 2-12 and Attachment A) is attributable to BINANCE ACCOUNT user ID number XXXX1716 which is held in the name of MO GUOPIAO. The records include the email address gosstechhr@gmail.com and the Republic of Singapore driving license bearing the name of MO GUOPIAO. The BINANCE ACCOUNT was opened on or about January 16, 2018.

63. The Defendant Cryptocurrency consists of the 87,637 USDT traceable to Victim-1's funds and transferred to the BINANCE ACCOUNT, transferred through several intermediary wallets identified in figures 2-11, and ultimately ending up in the BINANCE ACCOUNT, as shown in Attachment A.

## CONCLUSION

64. Based on my knowledge, training, and experience, and the foregoing information set forth in this affidavit, there is probable cause to believe that the Defendant Cryptocurrency is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C).

Pursuant to 28 U.S.C. § 1746, I declare under the penalties of perjury that the foregoing is true and correct to the best of my knowledge, information, and belief. Executed this 21 day of August, 2023.

Brian Christiansen, Special Agent
United States Secret Service